FILED

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA,
ALEXANDRIA DIVISION

2007 APR 26 A 10: 53

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

Project Honey Pot, a dba of Unspam Technologies, Inc.

Plaintiff,

v.

John Does Injuring PHP and its Members By Harvesting Email Addresses, Transmitting Spam, And Posting Comment Spam,

Defendants.

No. 1:07cv419
CMH/LO

PROJECT HONEY POT'S COMPLAINT FOR VIOLATIONS OF THE FEDERAL CAN-SPAM ACT AND THE VIRGINIA COMPUTER CRIMES ACT

1. Spam is a global problem of epidemic proportions, and the trend lines are headed in the wrong direction. By some estimates, spam now constitutes over 90% of all email traffic. Using vast networks of hijacked computers, counterfeiters, thieves and hi-tech snake-oil salesmen now have instant access to a global marketplace. No longer relegated to dark street corners, basement labs, and the trunks of seedy cars, illegal and dangerous products are now only a mouse click away from every Internet user. Spammers don't even need to have a product to sell to make money. Identity thieves, extortionists and phishers have opened Internet storefronts, and unwitting victims fall prey to them every day without ever leaving their living rooms. Children are also victimized by spam, which offers them easy access to illicit drugs, prescription drugs that need no prescription, gambling websites, pornography, fake IDs, spyware disguised as computer games, and a host of other temptations. Nation-states, too, are falling victim to spam

and the international criminal gangs that are increasingly behind it. Government corruption, failed legal systems and safe haven rules that generate a substantial portion of the nation-state's GDP all contribute to the problem, and are all being exploited by spammers.

2. A long list of laws prohibits spam. Perhaps the most elegant is the centuries old common law of trespass to chattels, which one judge in this District suggested fit the spam problem like a hand in glove. Notwithstanding that suggestion, a flurry of state and federal statutes has been passed over the last decade in an attempt to stop spam (or at least slow its growth) without unduly burdening "ham" (non-spammy email). The culmination of this legislative activity was the Federal CAN-SPAM Act of 2003 (15 U.S.C. § 7701 et seq.).

3. CAN-SPAM, it was hoped, would help stop spam by clarifying the rules that bulk emailers were supposed to follow. The reality is that legitimate emailers generally complied with CAN-SPAM long before it was enacted, or at least complied to the degree that the identity of someone who accepted responsibility for the mailing could be found on the face of the message itself. Spam is different. On its face, spam never identifies anyone willing to accept responsibility for the mailing. The reason is simple – spam violates the most basic standards of good conduct. Once identified, spammers cannot defend their "business" practices to anyone, let alone to an upstream webhost, email service provider or judicial fact finder.

4. If there were ever any doubt, today it is clear that the key to stopping spam is identifying those responsible for it, and getting that information into the hands of those willing and able to do something about it.

5. Discovering a spammer's identity is not simple, but it is not impossible either. To hide successfully, spammers have to do more than just avoid putting their name in their messages. Everything they do has to be anonymous; they have to hide while

simultaneously fooling their victims (and everyone else who is providing them with some service essential to their criminal enterprise) into thinking they are running a legitimate business.

6. The first thing a spammer needs is a long list of email addresses to spam. Spammers get your email address in two primary ways. They steal them (via harvesting) or they guess them (via dictionary attacks). The most common way spammers steal email addresses is by harvesting them from websites, using web spiders. This makes life difficult for the rest of us because posting email addresses on a website is a convenient way to facilitate communications between visitors to a website and the owners of the website. Owners of websites who want to display email addresses can obtain some protection from harvesters by installing a Project Honey Pot on their website, and displaying this Project Honey Pot logo on their website:[1]

MEMBER OF PROJECT HONEY POT
Spam Harvester Protection Network
provided by Unspam

The logo serves as a warning to harvesters that all of the email addresses displayed anywhere on the website are protected by Project Honey Pot and deters harvesters by putting them at legal risk if they spam any addresses harvested from the website.

7. Domain name owners who want to protect their email system from spam can obtain some protection by donating an MX record to Project Honey Pot, and then publicly disclosing the fact of their donation (but they should not disclose the specific MX record donated, as spammers will simply avoid this MX record and continue to send spam to MX

[1] The website for the logo can be found at http://www.projecthoneypot.org/how_to_avoid_spambots_5.php.

records not donated to PHP). By publicly disclosing their affiliation with Project Honey Pot, PHP members warn spammers that their domain names are protected by Project Honey Pot.

Project Honey Pot, a dba of Unspam Technologies, Inc.

8. Project Honey Pot (www.projecthoneypot.org) is a distributed network of spam-tracking honey pots. The project allows spammers, phishers, and other e-criminals to be tracked throughout the entire "spam cycle." On information and belief, Project Honey Pot was the first distributed e-mail harvesting research effort linking those that gather e-mail addresses by scraping websites with those that send unsolicited and frequently fraudulent messages. Tens of thousands of users from at least 100 countries actively participate in Project Honey Pot's effort to track criminals who break the law via email. Project Honey Pot was created by Unspam Technologies, Inc (www.unspam.com) – an anti-spam company with the singular mission of helping design and enforce effective anti-spam laws. Unspam Technologies, Inc. is a Delaware corporation with its principal place of business at 1901 Prospector Ave., Suite #200, Park City, Utah 84060.

9. Project Honey Pot receives MX record donations from the owners of Internet domain names. Through those donations, email messages addressed to any username hosted at a donated domain name are directed to email servers owned and maintained by Project Honey Pot, and those email messages are then processed by and stored on computer equipment owned and maintained by Project Honey Pot. Project Honey Pot also makes available to Internet website owners email address honey pots that can be installed on their webpages. When a harvester visits those webpages looking for email addresses to steal, the harvester is handed a unique email address hosted within Project Honey Pot's distributed network of donated MX records. The harvester's IP address, the date and time of the visit and other characteristics of the

harvester are recorded by Project Honey Pot and maintained for analysis and tracking. When a spam message is received thereafter at the unique email address, Project Honey Pot can tie the spam message (and the spammer) to the harvester that was given that email address.

10. Project Honey Pot is currently monitoring over 2.1 million honey pot addresses for annoying spam and dangerous phishing messages. Between January 2005 and April 2007, John Doe spammers transmitted over 6.1 million spam messages to tens of thousands of unique email addresses belonging to PHP members that have donated an MX record to, and are receiving anti-spam protection from, Project Honey Pot. All of these email addresses were illegally harvested by the spammer (or one of his co-conspirators) from a website hosting a PHP honey pot, or were the subject of dictionary spam attacks that indiscriminately targeted random usernames hosted within Internet domain names that have donated an MX record to, and are receiving anti-spam protection from, Project Honey Pot.

11. To date, Project Honey Pot has identified 2,489,814 unique spam server IP addresses, 15,570 unique harvester IP addresses, 87,643 unique dictionary attack spam server IP addresses, and since April 2007, has identified 630 comment spam server IP addresses.

12. Every spam message transmitted to a Project Honey Pot honey pot email address harms Project Honey Pot. Each spam message is received by a mail server controlled by and paid for by Project Honey Pot, which then must process, store and analyze the message to help protect the website owners who have installed honey pots on their webpages from harvesters, and to protect the domain name owners who have donated MX records from spam attacks.

13. By this action, Plaintiff seeks: (i) an injunction to prevent further unlawful conduct; (ii) compensatory damages; (iii) punitive damages; (iv) attorneys' fees and costs of suit.

John Doe Defendants

14. Defendants' identity is currently unknown to Plaintiff because Defendants have intentionally acted to hide their identity to evade detection.

JURISDICTION AND VENUE

15. This action arises out of Defendants' violation of the Federal CAN-SPAM Act. The Court has subject matter jurisdiction of this action based on 28 U.S.C. § 1331.

16. Pursuant to 28 U.S.C. § 1391(b), venue is proper in this judicial district. A substantial part of the events or omissions giving rise to Plaintiff's claims, together with a substantial part of the property that is the subject of Plaintiff's claims, are situated in this judicial district. For example, 166 PHP members self-report they are located in Virginia. PHP members have installed honey pots on 175 websites that are located in Virginia, and these Virginia-based honey pots have distributed 36,402 email addresses to identified harvesters world-wide. In addition to PHP's substantial presence in Virginia, the John Does also have substantial connections to Virginia. For example, the John Doe spammers have used 111 harvester IP addresses in Virginia to harvest 848 PHP member honey pot email addresses. The John Does have also used 20,778 spam server IPs located in Virginia to transmit 60,143 spam messages to PHP member honey pot email addresses. And on 245 occasions, the John Does have relied entirely on Virginia IP addresses to further their illegal enterprise – by harvesting a PHP member email address from a Virginia-based IP address and then sending spam to that address from a spam server using a Virginia-based IP address. In addition, the webpages advertised in the spam messages were all visible in Virginia, and (on information and belief) many of the products and services advertised in the spam messages were shipped or delivered to physical addresses in Virginia.

17. The federal District Court for the Eastern District of Virginia has personal jurisdiction over Defendants based on the following facts: Defendants initiated emails from the Eastern District of Virginia, gained unauthorized access to computer servers located in the Eastern District, caused tortious injury in the Eastern District, and conducted business in the Eastern District of Virginia.

COUNT I
Violation of the Federal CAN-SPAM Act (15 U.S.C. § 7701 et seq.)

18. Plaintiff repeats and re-alleges the allegations in paragraphs 1 through 17 of this Complaint.

19. Defendants initiated the transmission, to a protected computer, of a commercial electronic mail message that contained, or was accompanied by, header information that was materially false or materially misleading, in violation of 15 USC § 7704(a)(1).

20. In a pattern or practice, Defendants initiated the transmission to a protected computer of a commercial electronic mail message that did not contain a functioning return electronic mail address or other Internet-based mechanism, clearly and conspicuously displayed, that a recipient could use to submit, in a manner specified in the message, a reply electronic mail message or other form of Internet-based communication requesting not to receive future commercial electronic mail messages from that sender at the electronic mail address where the message was received, in violation of 15 USC § 7704(a)(3).

21. In a pattern or practice, Defendants initiated the transmission of a commercial electronic mail message to a protected computer and failed to provide: (i) clear and conspicuous identification that the message was an advertisement or solicitation; (ii) clear and conspicuous notice that the recipient could decline to receive further commercial electronic mail

messages from the sender; and (iii) a valid physical postal address of the sender, in violation of 15 USC § 7704(a)(5).

22. Plaintiff is an Internet access service adversely affected by the above violations, and is entitled to an injunction barring further violations, statutory damages of $100 for every attempted transmission of a spam message that contains false or misleading transmission information, statutory damages of $25 for every attempted transmission of a spam message that otherwise fails to comply with the Federal CAN-SPAM Act, treble damages resulting from Defendants' use of email harvesters and dictionary attacks to facilitate their violations of the CAN-SPAM Act, and attorney fees and costs, as authorized by 15 USC § 7706(g).

COUNT II
Violation of Virginia's Anti-Spam Statute (18 Va. Code § 18.2-152.3:1 et seq.)

23. Plaintiff repeats and re-alleges the allegations in paragraphs 1 through 22 of this Complaint.

24. Defendants used a computer or computer network with the intent to falsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of bulk electronic mail through or into the computer network of an electronic mail service provider or its subscribers.

25. Defendants' transmissions were in contravention of the authority granted by or in violation of the policies set by Plaintiff. Defendants had knowledge of the authority or policies of those email service providers, or the authority or policies were available on Project Honey Pot's website.

26. As a result of Defendants' actions, Plaintiff has suffered injury, and is entitled to an injunction, and to recover actual damages, or in lieu thereof $1 for each and every

unsolicited bulk electronic mail message transmitted in violation of the statute, or $25,000 per day any offending message was transmitted, plus attorneys' fees and costs of suit.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests entry of judgment in its favor and against Defendants:

1. Granting preliminary and permanent injunctive relief against Defendants, and all those in privity or acting in concert with Defendants, enjoining them from directly or indirectly violating the terms of the CAN-SPAM Act or the terms of the Virginia anti-spam statute;

2. Awarding Plaintiff compensatory and punitive damages in an amount to be proven at trial;

3. Awarding Plaintiff attorneys' fees and costs associated with prosecuting this action; and

4. Granting Plaintiff such other or additional relief as this Court deems just and proper under the circumstances.

Dated: April 26, 2007

Respectfully submitted,

Jon Praed

INTERNET LAW GROUP

Jon L. Praed (VSB #40678)
4121 Wilson Boulevard, Suite 101
Arlington, Virginia 22203
(703) 243-8100

Attorneys for Plaintiff Project Honey Pot, a dba of Unspam Technologies, Inc.